UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DENISE LYMAN,

Plaintiff,

-v-

NEW YORK CITY HEALTH AND HOSPITALS CORPORATION,

Defendant.

STIPULATION AND ESI PROTOCOL

CIVIL ACTION NO.: 20-CV-4390 (PAE) (SLC)

This Protocol (the "Protocol") governs the search, processing and production of Electronically Stored Information ("ESI") by and among Plaintiff Denise Lyman and Defendant New York City Health and Hospitals Corporation, each of whom individually is referred to herein as a "Party," and collectively, the "Parties," during the pendency of this litigation.

The Parties and their attorneys do not intend by this Protocol to waive their rights to the attorney work-product privilege or any other privilege. The Parties preserve their attorney-client privileges and other privileges, all of which are preserved and protected to the fullest extent provided by law, and there is no intent by this ESI Protocol, or the production of Documents pursuant to this ESI Protocol, to in any way waive or weaken these privileges. Documents produced hereunder are fully protected and covered by any protective order entered by this Court and orders of the Court effectuating same. The Parties do not waive any objections to the discoverability, admissibility, or confidentiality of Documents or ESI. Nothing in this Order shall be interpreted to supersede the provisions of any protective order governing confidentiality and/or privilege entered by the Court in this litigation, unless expressly provided for in such an order. The Parties shall comply with this ESI Protocol to the extent reasonably feasible. A Party is not required to comply with any aspect of this Protocol that is unreasonable or infeasible

provided that it informs the other Party in writing at or before the time of production as to why compliance with the Protocol is unreasonable or infeasible.

1. DEFINITIONS

1.1. "Requesting Party" means and refers to the Party that serves a request for the production of Documents.

1.2. "Producing Party" means and refers to the Party upon whom a request for the production of Documents is served.

1.3. "Document" or "Documents" means writings, including typewriting, printing, photographing, photocopying, transmitting by electronic mail or facsimile, any form of communication or representation, including letters, words, pictures, sounds or symbols or combinations thereof, and any record created thereby using Electronically Stored Information.

1.4. "Electronically stored information" or "ESI" means any Document or Documents stored or transmitted in electronic form.

1.5. "Native Format" means and refers to the format of ESI in which it was generated and/or as used by the Producing Party in the usual course of its business and in its regularly conducted activities. For example, the Native Format of an Excel workbook is a .xls or .xslx file.

1.6. "Metadata" means the information associated with each Document that is identified in Attachment A.

1.7. "Optical Character Recognition" or "OCR" means the process of recognizing, and creating a file containing, visible text within an image.

1.8. "Hash Value" is a unique numerical identifier that can be assigned to a file, a group of files or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the text contained within the file or files.

1.9. "Confidentiality Designation" means the "Confidential" legend affixed to Documents, as defined by, and subject to, the terms of the Protective Order entered in this matter.

1.10. "Searchable Text" means the text extracted or generated using OCR from any Document that allows the Document to be electronically searched.

1.11. "Load Files" means electronic files provided with a production set of Documents and images used to load that production set into a Requesting Party's Document review platform.

1.12. "Include" and "Including" shall be construed to mean "include but not be limited to" and "including, but not limited to".

1.13. "All" and "each" shall both be construed as all and as each.

2. IDENTIFICATION OF RESPONSIVE DOCUMENTS

2.1. The producing party may apply electronic searches in order to identify potentially responsive ESI. The producing party will disclose the search protocol that it intends to utilize for such searches, comprising, as appropriate, (a) the custodians and/or sources of ESI that are to be searched; (b) the search terms to be applied against those custodians and/or sources; (c) the date range to be applied against those custodians and/or sources; and (d) any other search criteria to be used to identify potentially responsive ESI (*e.g.*, technology assisted review ("TAR")). The requesting party may propose reasonable modifications to the search protocol, and to the extent there is a dispute, the parties will follow Judge Cave's rules regarding discovery disputes.

2.2. The producing party has the right to fully review its ESI for responsiveness, privilege, confidentiality, and personally identifiable information ("PII") prior to production of responsive, non-privileged documents.

3. PROCESSING SPECIFICATIONS FOR ESI

3.1. De-Duplication. A Producing Party may remove Documents identified as duplicative based on MD5 or SHA-1 hash values of the full text of the Documents at the family level across custodians and sources. The Producing Party shall produce a Metadata field for all produced Documents for which duplicate Documents were removed listing the Custodians that possessed a duplicate Document that was removed. The Producing Party will update this field no later than 10 days following substantial completion of production. The above shall not impose on a Party any obligation to produce duplicative Documents.

3.2. E-mail Threading. The Parties are permitted to use commercially reasonable e-mail threading tools to remove e-mails and their attachments where the contents of the e-mail and its attachments are wholly included within another e-mail that is not removed.

3.3. De-NISTing. Non-user-generated files may be removed from review and production using the list of non-user-generated files maintained by the National Institute of Standards and Technology (NIST). Additional culling of system files based on file extension may include: WINNT, LOGS, DRVS, C++ Program File (c), C++ Builder 6 (cpp), Channel Definition Format (cdf), Creatures Object Sources (cos), Dictionary file (dic), Executable (exe), Hypertext Cascading Style Sheet (css), JavaScript Source Code (js), Label Pro Data File (IPD), Office Data File (NICK), Office Profile Settings (ops), Outlook Rules Wizard File (rwz), Scrap Object, System File (dll), temporary files (tmp), Windows Error Dump (dmp), Windows Media Player Skin Package (wmz), Windows NT/2000 Event View Log file (evt), Python Script files (.py, .pyc, .pud, .pyw), Program Installers.

3.4. Embedded Objects. Files that are embedded in other files ("Embedded Objects"), including email inline images and Microsoft Office embedded images, need not be extracted as

separate files and treated as attachments to the parent Document provided that all content contained in the Embedded Object is contained and/or visible within the parent Document, to the extent it is produced. However, any embedded Documents that contain privileged material will be redacted and produced as separate attachments.

3.5. Searchable Text. Text will be extracted directly from the native electronic file of ESI unless the Document requires redaction, is an image file or is any other native electronic file that does not contain text to extract (*e.g.*, non-searchable PDFs), in which case Searchable Text may be created using OCR. Extracted text will include all comments, revisions, tracked changes, speaker's notes and text from Documents with comments or tracked changes, and hidden worksheets, slides, columns and rows. Extracted text from e-mails will include all header information that would be visible if the e-mail was viewed natively including: (1) the individuals to whom the communication was directed, (2) the author of the e-mail communication, (3) who was copied and blind copied on such e-mail, (4) the subject line of the e-mail, (5) the date and time of the e-mail and (6) the names of any attachments.

3.6. Exception Files. The Parties will use commercially reasonable efforts to address Documents that present processing or production problems (including encrypted, unsupported, and/or protected files) ("Exception Files"). A Party is not required in the first instance to produce Exception Files it has been unable to resolve through commercially reasonable efforts, except that, upon reasonable request, the Producing Party will undertake reasonable efforts to locate passwords for specifically identified Documents. Exception Files that are attached to produced Documents will be produced as a Bates-stamped placeholder TIFF bearing the legend, "This Document was unable to be processed".

4. PRODUCTION FORMAT

4.1. General. Except as otherwise provided herein, the Parties will produce Documents in TIFF Format. Spreadsheets (*e.g.*, Excel files), audio and video files shall be produced in Native Format. A Requesting Party may request the production of Native Files of other Documents (*e.g.*, images) where the production of the Native File is reasonably necessary to the Document's comprehension or use.

4.2. Confidentiality. The producing party shall designate Documents containing "Confidential" material, as defined by, and subject to, the terms of the Protective Order entered in this matter, in the following manner: (i) stamping or otherwise clearly marking Documents with a "CONFIDENTIAL" legend in a manner that will not interfere with legibility or audibility; and (ii) identifying the Confidential Material as "CONFIDENTIAL" in the "DESIGNATION" data field for all productions.

4.3. TIFF Format. All TIFFs produced by any party in this matter will be single-page Group IV TIFF format with 300 dpi quality or better. TIFF files will be named according to the corresponding Bates numbered images. All Documents that contain comments, deletions and revision marks (including the identity of the person making the deletion or revision and the date and time thereof), speaker notes or other user-entered data that the source application can display to the user will be processed such that all that data is visible in the image. All TIFF images will be branded in the lower right-hand corner with its corresponding Bates number, and in the lower left-hand corner with its Confidentiality Designation, if any, using a consistent font type and size.

4.4. Native Format. For Documents produced in Native Format, a Bates-stamped placeholder TIFF bearing the legend "This Document has been produced in Native Format" shall

also be produced in the same manner as other TIFFs. Native Files shall have a file name that includes the Bates number. Any Party printing the Native File for use in this matter shall append and use the placeholder TIFF as a cover sheet to the Native File at all times.

4.5. Load Files. Productions will include image load files in Opticon format and Concordance format data (.dat) files with reasonably available Metadata as identified in Attachment A for all Documents. All Metadata will be produced in UTF-7 or UTF-8 with Byte Order Mark format.

4.6. Text Files. A single document-level text file containing the Searchable Text shall be provided for each Document. The text file name shall be the same as the Bates number of the first page of the Document with the Document extension ".txt" suffixed. File names shall not have any special characters or embedded spaces. Searchable Text shall be provided in UTF-8 or Western European (Windows) with Byte Order Mark format text.

4.7. Databases, Structured, Aggregated or Application Data. For requests in which responsive information is contained in a database or other structured or aggregated data source or otherwise maintained by an application, the Parties will meet and confer to determine an appropriate format. If the Parties cannot reach agreement, the matter may be submitted to the Court for resolution pursuant to the Court's Individual Rules, at Paragraph 2.C, and Local Rule 37.2.

4.8. Redactions. Parties may redact information that is subject to the attorney-client privilege, work-product protection or any other protection from disclosure. Parties may also redact information that is personally or commercially sensitive, or implicates public safety concerns, so long as that information is not responsive to any agreed requests for production. Metadata for redacted Documents will include only the Bates number fields and the Custodian

field. Redacted Documents shall be identified as such in the Metadata. If a party redacts Documents for any reason, it will describe the reason for the redaction. For example, if a party redacts a Document to comply with privacy laws, it will stamp the words "REDACTED – PRIVACY" where the material originally appeared, on each page of the redacted Document. Redactions for privileged material should be stamped with the words "REDACTED – PRIVILEGE" or stamped with the reason for the privilege redaction, e.g. "attorney client communication", and appear in a log prepared pursuant to Instruction 5 below.

4.9. Color. All TIFFs will be produced in black and white. Upon reasonable request, the Producing Party will produce Documents in color on an as-needed basis to assist with readability.

4.10. Parent-Child Relationships. Parent-child relationships (the association between an attachment and its parent Document or between embedded Documents and their parent) will be preserved through the production of an appropriate Metadata field.

4.11. Family Groups. A Document and all other Documents in its attachment range, e-mails with attachments and files with extracted embedded OLE Documents all constitute family groups. Attachments that are wholly privileged or non-responsive may be excluded from production provided that a slipsheet with the placeholder "Document Withheld as Privileged" or "Non-Responsive Document" is produced. This information should also be reflected in the Contains Slip Sheet and Slip Sheet Language fields in the .DAT file. The receiving party may contact the producing party if the receiving party seeks additional information about certain excluded, non-responsive documents, and the producing party agrees, where reasonable, to provide an explanation as to the reason such documents are not responsive to the requests.

4.12. Production Media. The Producing Party will use the appropriate electronic media (CD, DVD, secure FTP or other secure file transfer utility, hard drive or other mutually agreeable media) for its production, and will use high-capacity media to minimize associated overhead. The Producing Party will label any physical media with the Producing Party, media volume name and Document number range.

5. PRIVILEGE LOG

5.1. The Producing Party will provide the Requesting Party with a log of the Documents withheld in full for privilege containing information sufficient to enable the Requesting Party to evaluate the claims made, including the following information to the extent reasonably available: Document Number, Custodian, Author/Sender, Recipient, CC Recipient, BCC Recipient, Date, Basis for Withholding (*e.g.*, Attorney-Client Communication) and Document Description. The parties will exchange privilege logs no later than 30 days following substantial completion of document discovery, and supplement that privilege log as necessary thereafter.

5.2. The same Document Description may be used for multiple Documents (*i.e.*, a categorical description) so long as the Producing Party has, in good faith, evaluated the Document to ensure the Document Description accurately reflects the contents of the Document and is sufficient for the Receiving Party to fairly evaluate the claim of privilege or immunity.

5.3. A single Document containing multiple e-mails in an e-mail chain may be logged as a single entry. A Document family (*e.g.*, e-mail and attachments) may be logged as a single entry so long as the log entry references the attachment(s) and accurately describes both the e-mail and its responsive attachment(s).

5.4. A party is not required to log redacted Documents provided that it states the reason for the redaction in the text of the redaction box (*e.g.*, Attorney-Client Privilege, Work Product, Personally Sensitive, Commercially Sensitive).

5.5. The Parties are not required to log privileged Documents created after the initiation of litigation in this matter on June 2, 2020.

6. GENERAL PROVISIONS

6.1. Any practice or procedure set forth herein may be varied by agreement of the Parties, which will be confirmed in writing.

6.2. The Parties will meet and confer in an attempt to resolve any dispute regarding the application of this Protocol before seeking Court intervention.

Dated: August 6, 2021

GEORGIA M. PESTANA
Corporation Counsel of the City of New York

By: /s/ Alana Rachel Mildner
Alana Rachel Mildner
Assistant Corporation Counsel
100 Church Street
New York, NY 10007
Tel.: (212) 356-1177
amildner@law.nyc.gov

Attorney for Defendant New York City Health and Hospitals Corporation

CRAVATH, SWAINE & MOORE LLP

/s/ Carolyn Young
Carolyn Young
Worldwide Plaza
825 Eighth Avenue
New York, NY 10019
Tel: (212) 474-1865
cyoung@cravath.com

Attorney for Plaintiff Denise Lyman

SO ORDERED:

Dated: 8/9/2021
New York, New York

SARAH L. CAVE
United States Magistrate Judge

ATTACHMENT A

FIELD NAME	DESCRIPTION	EXAMPLE
Production Begin	Starting Bates number of file	NYCE00000001
Production End	Ending Bates number of file	NYCE00000005
Production Begin Family	Starting Bates number of family	NYCE00000001
Production End Family	Ending Bates number of family	NYCE00000010
Page Count	Number of pages in the file	6
Native Link	Hyperlink to native file	Z:\VOL001\NATIVES\00\NYCE00000001.doc
All Custodians	All custodians of the record, if global deduplication was applied during processing. A revised ALLCUSTODIANS field must be provided in the form of an overlay for any documents affected by new custodians added to the database post-production.	Doe, John;Smith, Mary;Robinson, Jane
File Path	Original path of the file	Path\Folder2\My Documents
File Name	Name of the file	My Meeting.doc
File Extension	Extension of the file	DOC
File Type	Classification assigned by the processing software	Microsoft Word Document
Title	Data stored in the title metadata field	Agenda for Weekly Meeting
Author	Data stored in the author metadata field	jdoe
Subject	Subject of the email or the data stored in the subject metadata field	Meeting Agenda
From	Email address and display name of the sender of the email	John Doe <jdoe@company.com>
To	Email address(es) and display name(s) of the recipient(s) of the email	Frank Smith <frank.smith@mycompany.com>;Jane Doe <jane.doe@mycompany.com>
CC	Email address(es) and display name(s) of the CC(s) of the email	Joseph Roberts <jroberts@company.com>;Mark Smith <msmith@company.com>

BCC	Email address(es) and display name(s) of the BCC(s) of the email	Joseph Roberts <jroberts@company.com>;Mark Smith <msmith@company.com>
Attachment Names	List of files attached to email	File 1.xls;File 3.zip
Date Sent	Sent date of the email	09/15/2012
Time Sent	Sent time of the email (12hr format)	3:30:25 PM
Date Modified	Last modified date of the file as captured by the original application or the last modified date of the file as captured by the file system	09/09/2012
Time Modified	Last modified time of the file as captured by the original application or the last modified time of the file as captured by the file system (24hr format)	9:30:30 AM
Importance	Importance property of email	High
Sensitivity	Sensitivity property of email	Confidential
MD5 hash	MD5 hash of file	D41D8CD98F00B204E9800998ECF8427E
Family Date	Sent date of the email or the last modified date of the parent document	09/15/2012
Family Time	Sent time of the email or the last modified time of the parent document (24hr format)	3:30:25 PM
Privilege Type	This field will indicate the reason for any redactions	ACC; AWP
Redaction Type	This field will indicate if the document contains a redaction	Privilege; PII; NR
Contains Slip Sheet	This field will indicate if the documents has been slip-sheeted	Yes
Slip Sheet Language	This field will indicate the language that appears on the slip-sheet	DOCUMENT WITHHELD FOR PRIVILEGE
Designation	This field will indicate any designations on the image besides the bates number	CONFIDENTIAL
Text Link	Hyperlink to text file	Z:\VOL001\TEXT\00\NYCE00000001.txt